

Chapter 2

VRP Basics

2.1 Introduction to VRP

Versatile Routing Platform (VRP) is a network operating system applied in Huawei network devices like routers and switches. It provides users of these network devices with a consistent and powerful configuration platform by standardizing network, user, and management interfaces. Communication engineers all over the world may have frequently used these Huawei devices, as Huawei has a large international deployment of network devices. It is required for these engineers to understand the basics of VRP.

Based on the TCP/IP model, VRP's hierarchical system architecture integrates device and network management capabilities, network application technologies, and data communication technologies, such as routing, multiprotocol label switching (MPLS), virtual private network (VPN), and security technologies, with a real-time operating system.

To ensure the configuration platform remains up-to-date and relevant for current technologies, VRP has evolved from VRP1.0, first released in 1998, to VRP8.X, its latest version.

Figure 2.1 illustrates the main features of each version.

Many of the low-end and mid-range network devices currently in use on enterprise networks run VRP5.X. As such, this book focuses on VRP5.12.

2.2 VRP Command Lines

VRP command lines are directly defined to configure and manage Huawei network devices. After completing this section, you should be able to:

- Describe the concepts, functions, and basic structure of a command line.
- Understand the differences between the user, the system, and the interface views.
- Understand command levels and user levels.
- Effectively use command lines.

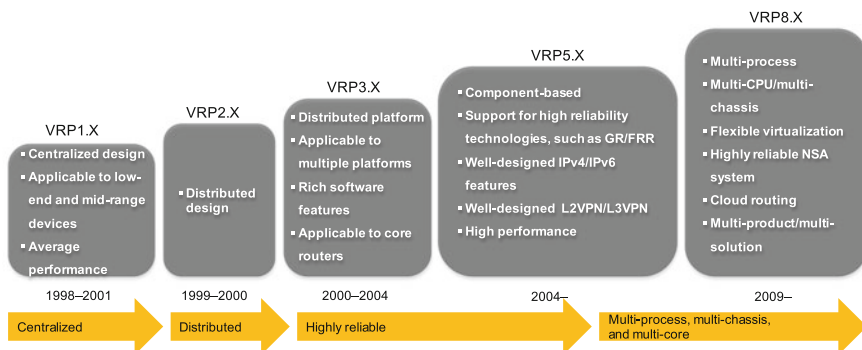


Fig. 2.1 VRP features by version

2.2.1 Basic Concepts

- Command line

VRP command lines are character strings used to configure functions and deploy services on Huawei network devices. A command line consists of keywords and parameters. Keywords are one or more words that uniquely identify, correspond to, and generally describe the instruction that a command line performs, and parameters specify the data that is used as input for the keywords. This book shows keywords in **bold** and parameters in *italic*. For example, in the command line **ping** *ip-address* (which tests a device's connectivity), **ping** is the keyword, and *ip-address* represents a user-specified parameter such as 192.168.1.1.

Huawei's network devices generally are shipped unconfigured by default, so the user must enter command lines in the device's command-line interface (CLI) to configure the functionality of the device.

- CLI

A CLI provides a means of interacting with a device. Through the CLI, you can enter command lines to configure devices. VRP command lines, of which there are thousands, are classified by function and registered in different command views.

- Command view

The CLI provides several command views, of which the user, the system, and the interface views are the most commonly used. To enter and use command lines in the CLI, you must first access the user view (as shown in Fig. 2.2). This view allows you to query a device's basic information and status and access other views, but does not allow service functions to be configured. You can configure service functions and run the basic configuration commands in the system view (as shown in Fig. 2.3), which can be accessed from the user view by running the **system-view** command.

The system view also allows you to access other views, such as the interface view (as shown in Fig. 2.4). In the interface view, you can configure parameters and services for a specified interface.

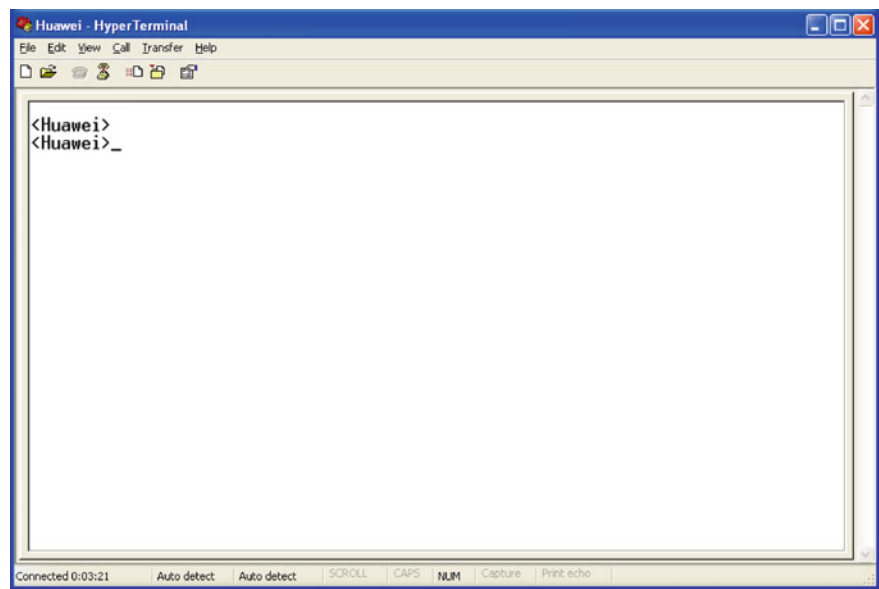


Fig. 2.2 User view interface

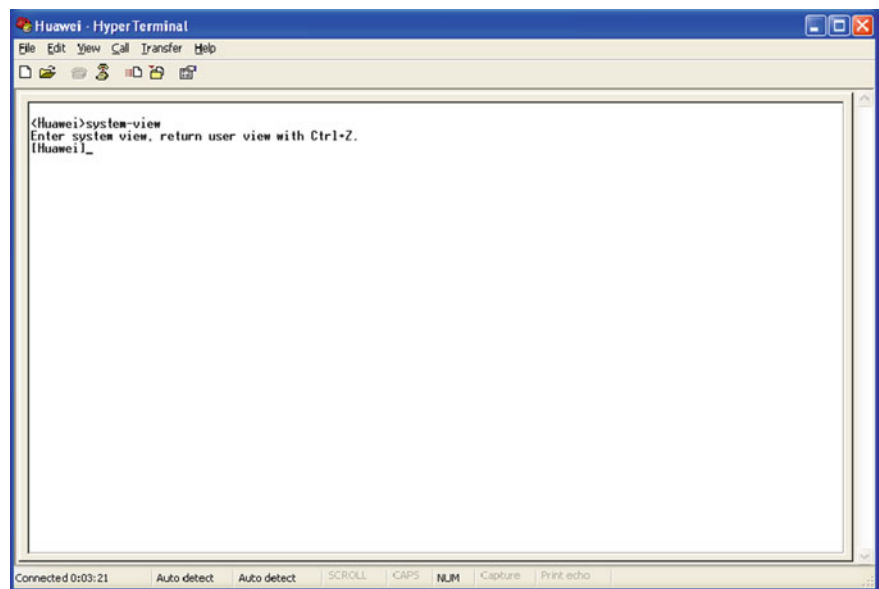


Fig. 2.3 System view interface

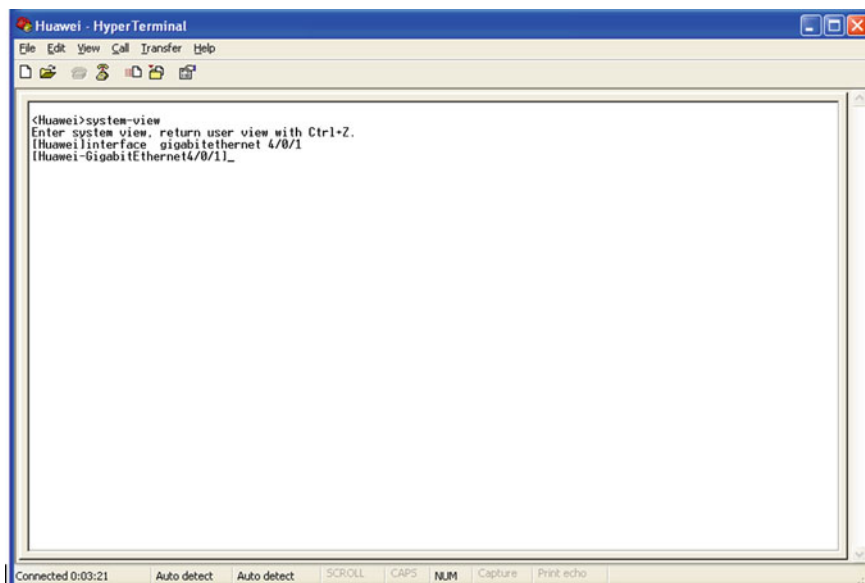


Fig. 2.4 Interface view interface

The command prompt in each view contains the device's host name ("Huawei" in the preceding figures), which in the user view is enclosed in angle brackets (`<...>`) and in all other views is enclosed in square brackets (`[...]`). In some views, the command prompt may contain additional information (such as the interface identifier, `GigabitEthernet4/0/1`, in the preceding interface view example).

- Command and user levels

VRP commands are classified based on the function they perform: Level 0 (visit level) commands test network connectivity, Level 1 (monitoring level) commands display network status and basic device information, Level 2 (configuration level) commands configure services for a device, and Level 3 (management level) commands manage certain functions of a device, such as uploading or downloading configuration files.

To limit which commands a user can run, users are assigned different user levels. In total, 16 user levels are available, from Level 0 to Level 15. Level 0 is the most restrictive, with the permissiveness increasing for each subsequent level. By default, Levels 4 through 15 are the same as Level 3, so users assigned these levels all have the same permissions and can run all VRP commands. However, user levels can be configured if finer granularity of control is required. For example, you can increase to Level 15 the user level of particular commands so that only users assigned this level can run these commands. However, changing the default assignments may complicate operation and maintenance tasks and weaken device security—consulting with Huawei engineers is advisable if you want to change these default assignments. Table 2.1 lists the default mapping between user and command levels.

Table 2.1 Default mapping between user and command levels

User Level	Command Level	Description
0	0	Commands for network diagnostics (such as ping and tracert) and remote login (such as telnet)
1	0, 1	Commands for system maintenance, such as display . Specific display commands, such as display current-configuration and display saved-configuration , are management-level commands (requiring a Level 3 user)
2	0, 1, 2	Commands for service configuration, such as routing commands
3–15	0, 1, 2, 3	Commands for controlling basic system operations, such as file systems, FTP download, user management, command level setting, and fault diagnostics

2.2.2 Using Command Lines

This section explains how to use VRP command lines.

- Accessing a command view
As mentioned in Sect. 2.2.1, the user view is the first view displayed after you enter VRP. If <Huawei> is displayed (and the cursor to the right of > is blinking), you are in the user view. In this view, you can run commands to query the device’s basic information and status. To configure an interface, for example, you need to access the system view and then access the interface view. The commands to do this are **system-view** and **interface interface-type interface-number**. The following shows how to access the interface view of GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] //The system view is displayed.
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] //The interface view is displayed.
```

- Exiting from the command view
The **quit** command allows you to exit from the current view and return to the upper-level view. In the preceding example, the current view is the interface view, and the system view is the upper-level view of the interface view. Running the **quit** command in the interface view will show the following.

```
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] //Returned to the system view.
To return to the user view, run the quit command again.

[Huawei] quit
<Huawei> //Returned to the user view.
```

Sometimes you may want to return to the user view without running the **quit** command multiple times. The **return** command allows you to directly return to the user view.

```
[Huawei-GigabitEthernet1/0/0] return
<Huawei> //Returned to the user view.
```

You can also use shortcut keys **Ctrl+Z** in any view to return to the user view.

- **Editing a command line**
You can enter up to 510 characters per command line. However, if you notice a mistake in a long command line, retyping potentially 510 characters would become laborious. Table 2.2 lists the common function keys, which are case-insensitive, for editing VRP command lines. Note that the cursor cannot move into the prompt (for example, [Huawei-GigabitEthernet1/0/0]), nor can the prompt be edited.
- **Entering partial keywords**
Command-line completion automatically fills in partially entered keywords if the system can find a unique match. For example, you can enter combinations such as **d cu**, **di cu**, or **dis cu** and press **Tab**, and the system will automatically display the **display current-configuration** command. **d c** and **dis c**, however, return no match because other commands, such as **display cpu-defend**, **display clock**, and **display current-configuration**, also correspond to these partial keywords.
- **Obtaining help**
Memorizing the thousands of VRP command lines can seem like a daunting prospect. The question mark (?) makes things easier. You can enter ? at any time to obtain online help. The help is classified as either full help or partial help.

Table 2.2 Function keys for editing VRP command lines

Key	Function
Backspace	Deletes the character to the left of the cursor
← or Ctrl+B	Moves the cursor one character to the left
→ or Ctrl+F	Moves the cursor one character to the right (only as far right as the end of the command)
Delete	Deletes the character highlighted by the cursor (characters following the deleted character all move one space to the left)
↑ or Ctrl+P	Displays the last historical command that was run. The system stores a list of historically run commands, allowing you to display them one at a time (press repeatedly to view earlier commands)
↓ or Ctrl+N	Displays the next most recent historical command in the stored list

Full help, for example, displays a list of commands available in the current view. Entering ? in the user view will display the following.

```
<Huawei> ?
User view commands:
  arp-ping          ARP-ping
  autosave          <Group> autosave command group
  backup            Backup information
  cd                Change current directory
  clear             Clear
  clock             Specify the system clock
  cls              Clear screen
  compare           Compare configuration file
  copy             Copy from one file to another
  debugging         <Group> debugging command group
  delete           Delete a file
  dialer           Dialer
  dir              List files on a filesystem
  display           Display information
  factory-configuration Factory configuration
  fixdisk          Try to restore disk
---- More ----
```

From the list, you can determine which command you need. For example, the **display** keyword is described as **Display information**. This keyword is contained in more than one command, so enter any letter to quit help, enter **display** and a space, and then enter ?. The following information is then shown.

```
<Huawei> display ?
accounting-scheme  Accounting scheme
acl               <Group> acl command group
actual           Current actual
ap              <Group> ap command group
bfd             Specify BFD(Bidirectional Forwarding Detection)
bgp            BGP information
binding         Display binding relation of profile
bridge-link     Bridge link
bridge-profile   Display Bridge profile
bridge-whitelist Bridge Whitelist
bssid-decode    Display bssid detail information
calibrate       Global calibrate
clock           Clock status and configuration information
config         System config
cpu-defend      Configure CPU defend policy
cpu-usage       Cpu usage information
current-configuration Current configuration
---- More ----
```

From this list, you can determine which keyword to pair with **display**. For example, running the **display current-configuration** command displays the current configurations of a device.

Partial help is ideal for when you already know part of the command line. For example, if you know **dis** for **display** and **c** for **current-configuration** but cannot remember the complete command line, use partial help. Entering **dis** and **?** shows the following.

```
<Huawei> dis?
      display  Display information
```

The only keyword that matches **dis** is **display**. To determine the second part of the command line, enter **dis**, a space, **c**, and **?**.

```
<Huawei> dis c?
Cellular                Cellular interface
calibrate                Global calibrate
capwap                  CAPWAP
channel                 Informational channel status and configuration
                        information
clock                   Clock status and configuration information
config                  System config
controller              Specify controller
cpos                    CPOS controller
cpu-defend              Configure CPU defend policy
cpu-usage               Cpu usage information
current-configuration   Current configuration
cwmp                    CPE WAN Management Protocol
```

A few keywords start with **c**; however, it is easy to determine that the required command line is **display current-configuration**.

- Using shortcut keys

Shortcut keys facilitate entering commands. Pre-defined shortcut keys are called system shortcut keys. Some of the commonly used system shortcut keys are listed in Table 2.3.

Table 2.3 Commonly used system shortcut keys

Key	Function
Ctrl+A	Moves the cursor to the beginning of the current line
Ctrl+E	Moves the cursor to the end of the current line
Esc+N	Moves the cursor down one line
Esc+P	Moves the cursor up one line
Ctrl+C	Stops a running function
Ctrl+Z	Returns to the user view
Tab	Provides command-line completion. Pressing Tab after entering a partial keyword automatically completes the keyword if the system finds a unique match

System shortcut keys cannot be modified; however, you can define your own (known as user-defined shortcut keys). User-defined shortcut keys can provide added convenience but may conflict with some commands—defining such keys is therefore not recommended.

2.3 Logging into a Device

A number of methods are available for logging into a device to configure it and check its status. After completing this section, you should be able to:

- Log into a device through a console port.
- Log into a device through a MiniUSB port (and install the required driver).

2.3.1 Log into a Device Through a Console Port

One of the login methods uses a network device's console port, which connects to a PC's serial port through a console cable. Figure 2.5 shows the appearance and structure of a console cable.

The following example describes how to log in through the console port.

1. Connect a PC and a network device through a console cable.
The D-type connector of a console cable connects to the PC's serial port, and the RJ-45 connector connects to the device's console port (Fig. 2.6).
2. Create a connection and specify a communication port.



NOTE

This example uses a PC running Windows XP.

Power on the PC and device. Choose **Start > Programs > Accessories > Communications > HyperTerminal** to start the HyperTerminal. Create a

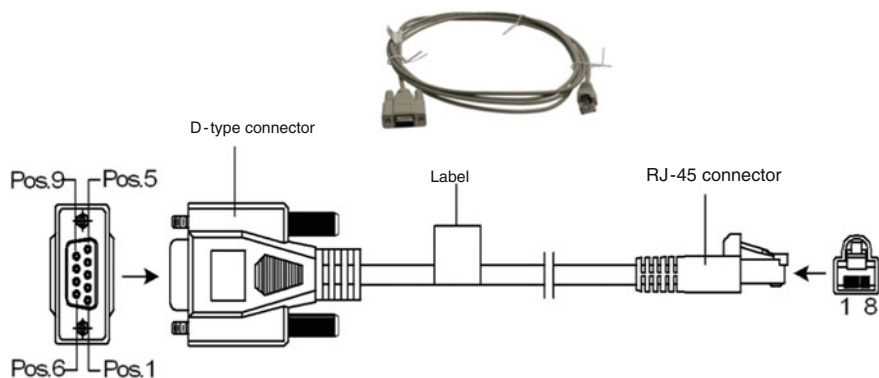


Fig. 2.5 Console cable

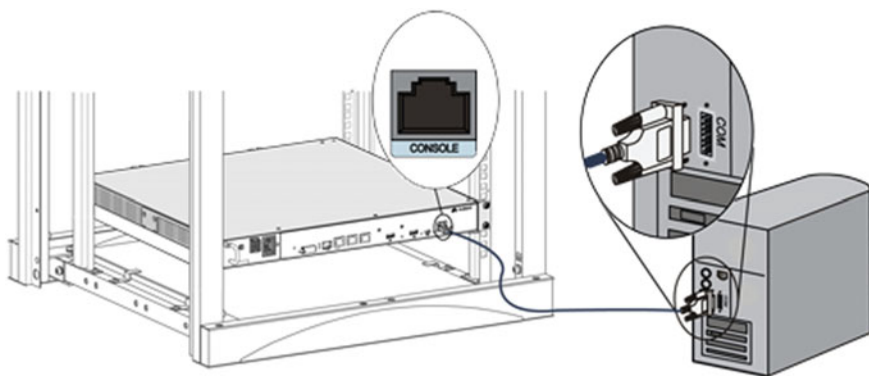


Fig. 2.6 Connecting a PC and network device through a console cable

connection (Fig. 2.7) and specify a communication port (Fig. 2.8). This example names the connection COMM1 and assumes that you connect the console cable to serial port COM1 on your PC.

3. Set communication parameters.

Communication parameters on both the PC and network device must be the same. All network devices that run VRP have the following default values:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Fig. 2.7 Creating a connection

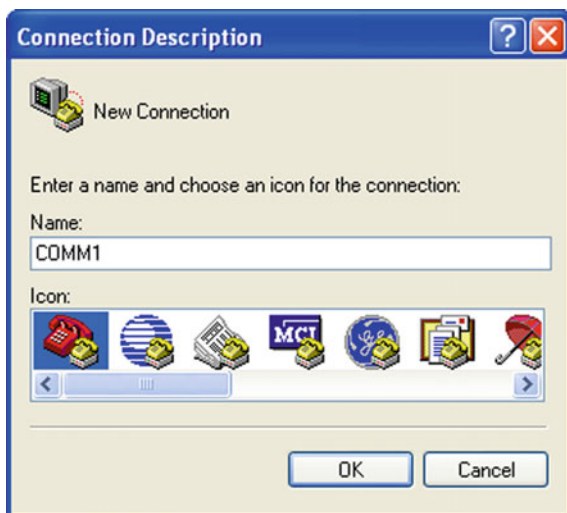
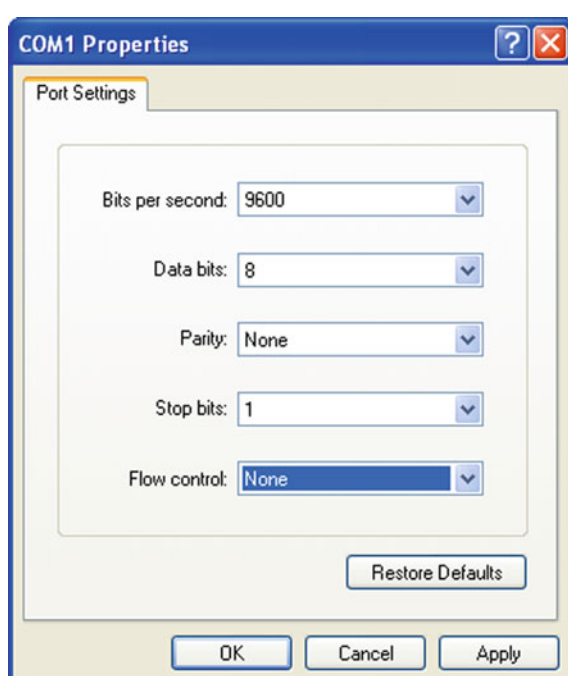


Fig. 2.8 Specifying a communication port



Fig. 2.9 Setting communication parameters



Windows XP also uses these values by default, so to use the default values on your PC, click **Restore Defaults**. Figure 2.9 shows the dialog box used to enter these values in Windows XP.

4. Enter the CLI.

In the dialog box shown in Fig. 2.9, click **OK** or press **Enter** to enter the CLI. If you are logging into the device for the first time, you will be prompted to configure a login password for the console port. After you configure a login password (for example, **huawei123**), the device prompts you whether to stop Auto-Config. If you want to manually configure the device, you must stop Auto-Config by entering **y**.

```
Please configure the login password (maximum length 16):huawei123
```

```
<Huawei>
```

```
Warning: Auto-Config is working. Before configuring the device, stop  
Auto-Config. If you perform configurations when Auto-Config is running, the  
DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop  
Auto-Config? [y/n]: y
```

```
<Huawei>
```

The device then displays `<Huawei>`, indicating that you have entered the user view from which you can run VRP command lines.

2.3.2 Log into a Device Through a MiniUSB Port

Another login method uses a network device's MiniUSB port, which connects to a PC's USB port through a MiniUSB cable. Figure 2.10 shows the appearance of a MiniUSB cable.

The following example describes how to log in through the MiniUSB port.

1. Connect a PC and network device through a MiniUSB cable.

The Type-A connector of a MiniUSB cable connects to the PC's USB port, and the Mini-B connector connects to the device's MiniUSB port (Fig. 2.11).

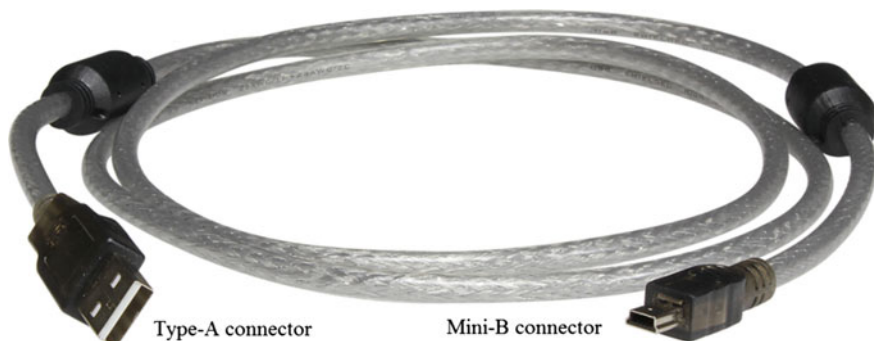


Fig. 2.10 Appearance of a MiniUSB cable

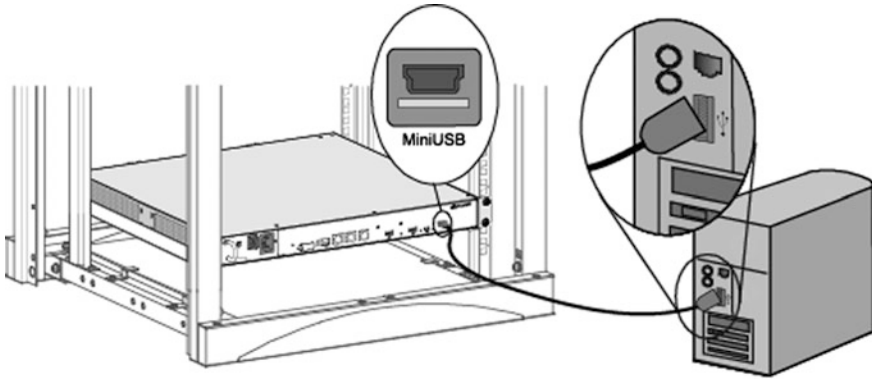


Fig. 2.11 Connecting a PC and network device through a MiniUSB cable

2. Install the MiniUSB driver.

NOTE

This example uses a PC running Windows XP.

The MiniUSB driver enables communication between the PC and device. To install the driver on your PC, perform the following steps:

- Step 1 Download the MiniUSB driver AR_MiniUSB_driver from <http://support.huawei.com/enterprise>. The driver is compatible with Windows XP, Windows Vista, and Windows 7. After the download is complete, double-click the driver installation file, and then click **Next** in the displayed **InstallShield Wizard** dialog box (Fig. 2.12).
- Step 2 Select the **I accept the terms in the license agreement** check box after reading and confirming you agree to the terms and click **Next** (Fig. 2.13).
- Step 3 In the **Destination Folder** dialog box, click **Change** to change the driver directory (if required), and then click **Next** (Fig. 2.14).
- Step 4 Click **Install** to decompress the driver (Fig. 2.15). After the system finishes decompressing the driver, click **Finish** (Fig. 2.16).
- Step 5 Navigate to the file decompression path and open the folder DISK1 (Fig. 2.17).
- Step 6 Double-click **setup.exe**, and in the displayed **InstallShield Wizard** dialog box, click **Next** (Fig. 2.18).
- Step 7 Select the **I accept the terms in the license agreement** check box after reading and confirming you agree to the terms and click **Next** to install the driver (Fig. 2.19).
- Step 8 After the installation is complete, click **Finish** (Fig. 2.20).
- Step 9 To confirm that the driver is successfully installed, right-click **My Computer** and choose **Computer Management > Device Manager > Ports (COM & LPT)**. If **TUSB3410 Device** is shown, the driver is installed successfully (Fig. 2.21).

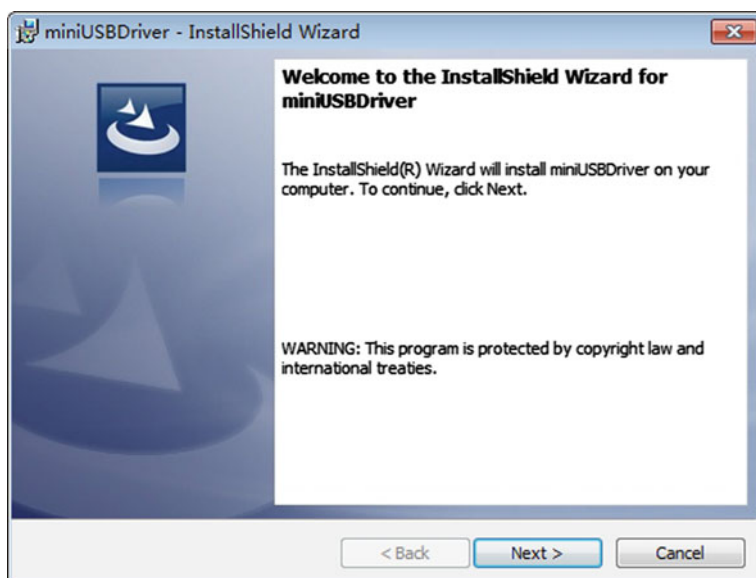


Fig. 2.12 InstallShield Wizard dialog box

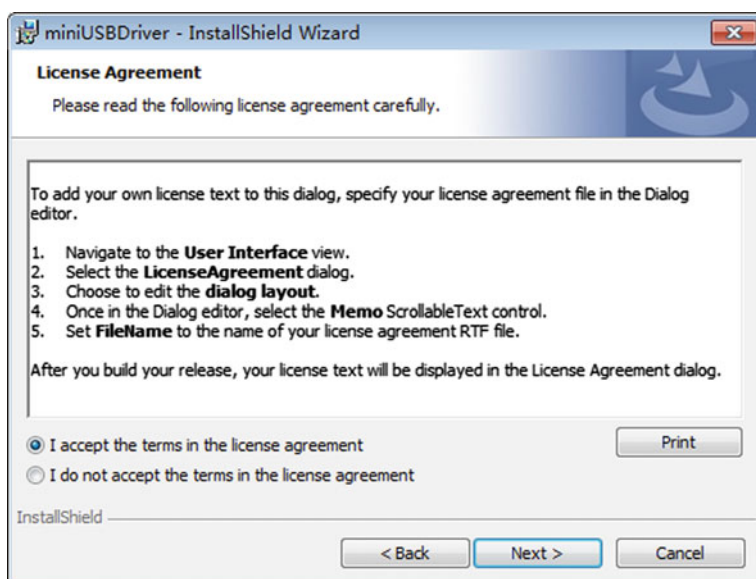


Fig. 2.13 License Agreement dialog box

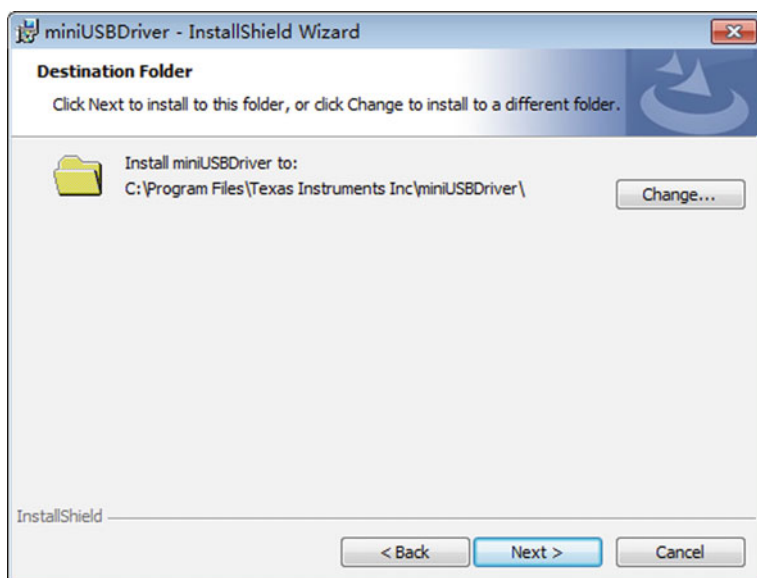


Fig. 2.14 Selecting the installation path

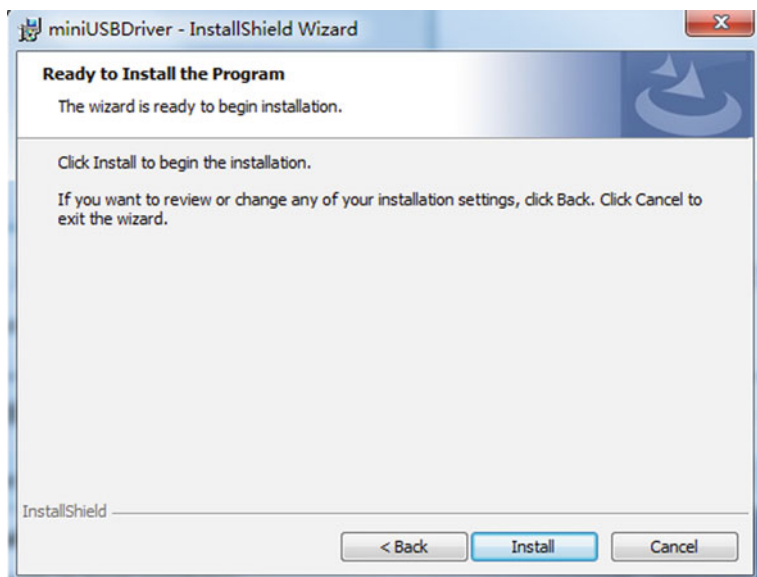


Fig. 2.15 Decompressing the driver

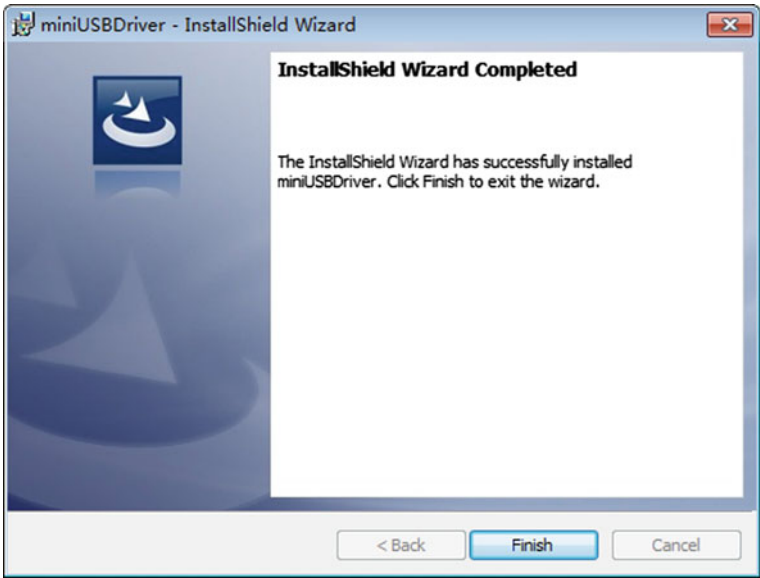


Fig. 2.16 Finishing driver decompression

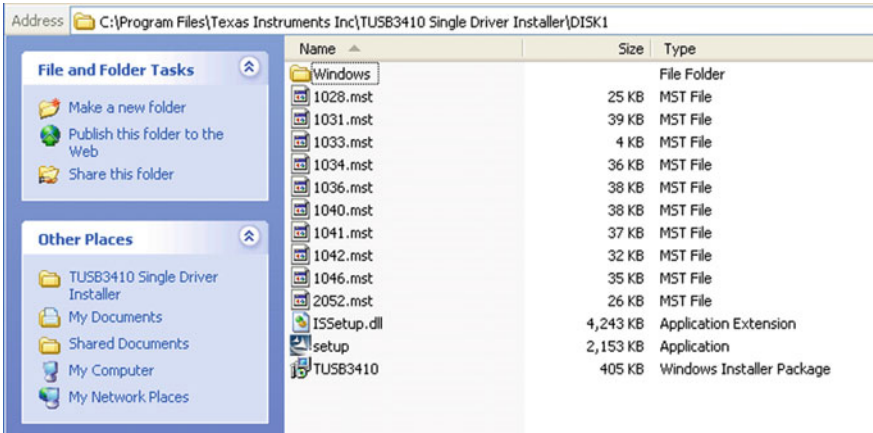


Fig. 2.17 DISK1 folder

1. Create a connection and specify a communication port.
Choose **Start > Programs > Accessories > Communications > HyperTerminal** to start the HyperTerminal. Create a connection (Fig. 2.22) and specify a

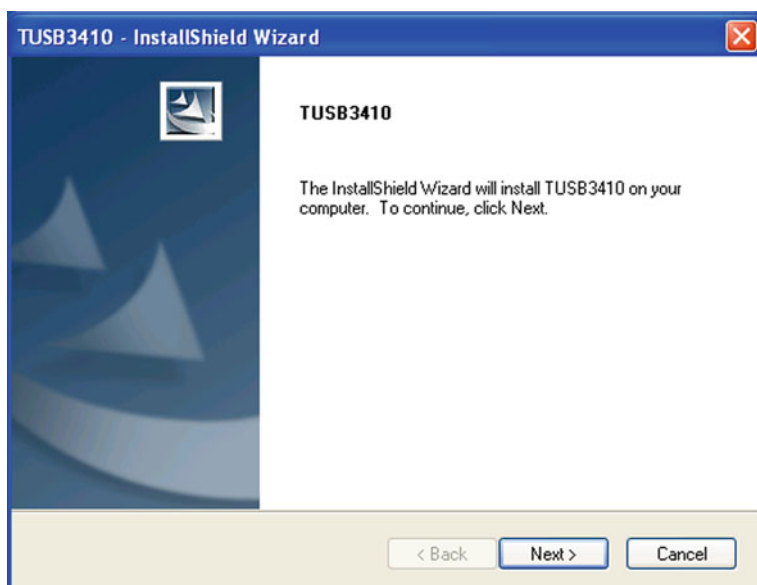


Fig. 2.18 InstallShield dialog box

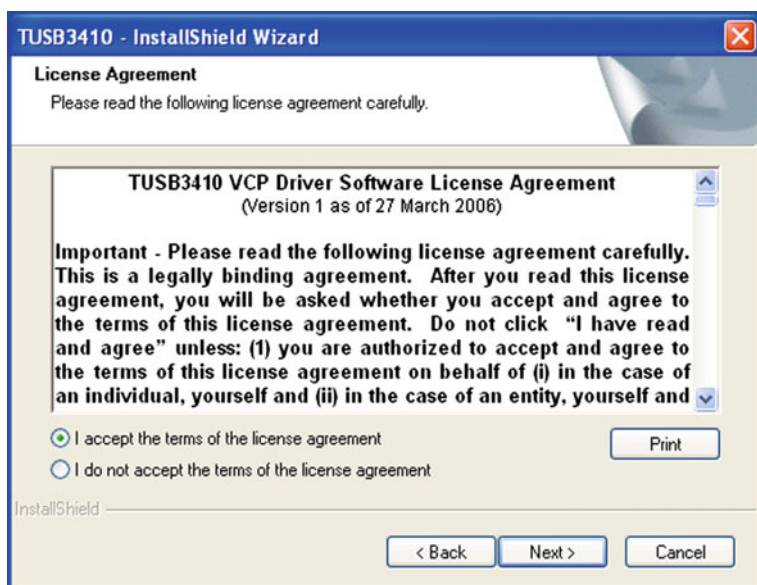


Fig. 2.19 License Agreement

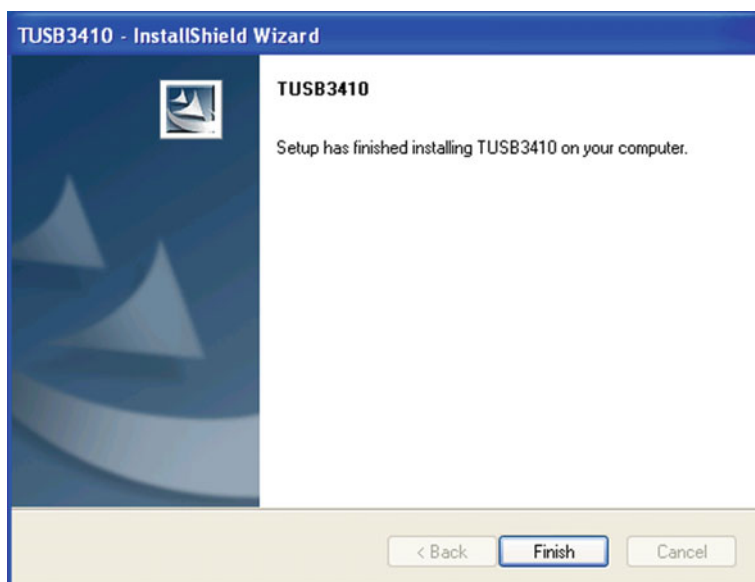


Fig. 2.20 Completing the installation

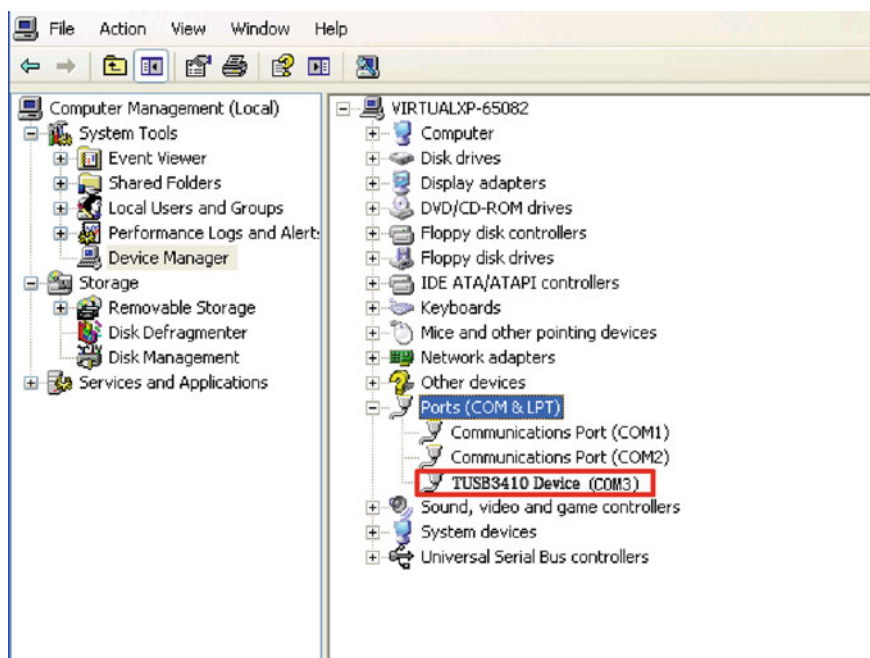


Fig. 2.21 Confirming the driver installation

communication port (Fig. 2.23). This example names the connection MiniUSB and specifies COM3 as the communication port.

2. Set communication parameters.

Communication parameters on both the PC and network device must be the same. All network devices that run VRP have the following default values:

Fig. 2.22 Creating a connection

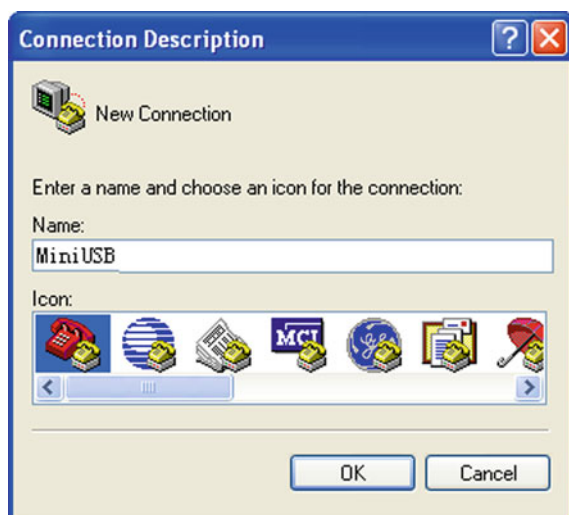
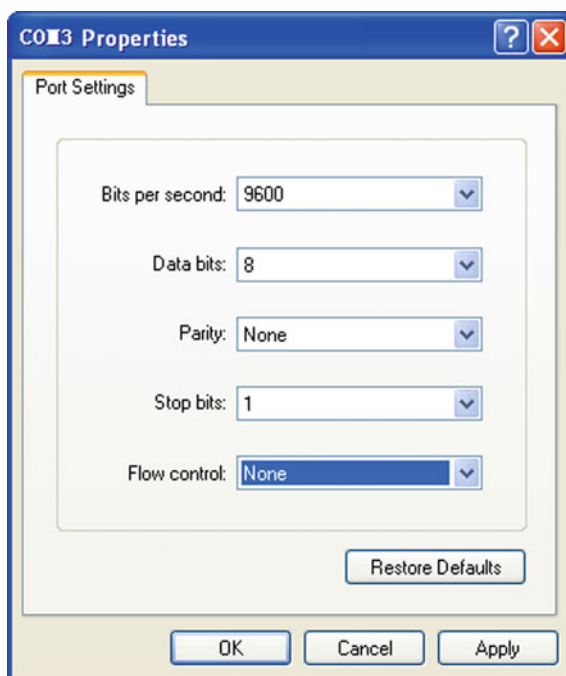


Fig. 2.23 Specifying a connection port



Fig. 2.24 Setting communication parameters



- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Windows XP also uses these values by default, so to use the default values on your PC, click **Restore Defaults**. Figure 2.24 shows the dialog box used to enter these values in Windows XP.

3. Enter the CLI.

In the dialog box shown in Fig. 2.24, click **OK** or press **Enter** to enter the CLI.

2.4 Basic Configurations

Huawei's network devices generally are shipped unconfigured by default, so to use a device you must first configure some of its basic functions. After completing this section, you should be able to:

- Set the host name.
- Set the system time.
- Configure IP addresses.
- Configure the user interface.

2.4.1 Setting the Host Name

In the CLI, the host name (the name of the device) is enclosed in angle brackets (`<...>`) or square brackets (`[...]`). The default host name is **Huawei**, but this name should be changed so that multiple devices can be better differentiated. To change the host name, use the **sysname** *host-name* command.

The following example shows how to change the host name to **Huawei-AR-01**.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] sysname Huawei-AR-01
[Huawei-AR-01]
```

2.4.2 Setting the System Time

By default, Huawei devices use Coordinated Universal Time (UTC). To specify a different time zone for a device, run the **clock timezone** *time-zone-name* {**add** | **minus**} *offset* command. You can name the time zone in the *time-zone-name* parameter, and specify whether the time zone's offset to UTC is positive (**add offset**) or negative (**minus offset**). Note that {*...*} indicates that one of the enclosed parameters must be selected. For example, if you want to set the time zone of the device as Beijing time, run the following command:

```
[Huawei-AR-01] clock timezone BJ add 08:00
```

After setting the time zone, run the **clock datetime** *HH:MM:SS YYYY-MM-DD* command to set the time and date. The *HH:MM:SS* parameter specifies the time, in 24-hour format, and *YYYY-MM-DD* specifies the date. (Huawei devices support only the 24-hour format.) For example, to set a time and date of 18:30 on March 10, 2015, run the following command:

```
[Huawei-AR-01] clock datetime 18:30:00 2015-03-10
```

2.4.3 Configuring an IP Address for the Device

In addition to the login methods described in Sect. 2.3, you can also use Telnet to log into a device. However, Telnet requires that an IP address be set on the device's interface. To set an IP address, run the **ip address** *ip-address* {*mask* | *mask-length*} command in the interface view. The *ip-address* and *mask* parameters specify the IP address and subnet mask, respectively, in dotted decimal notation, and *mask-length* specifies the number of consecutive "1"s in the binary notation of the subnet mask.

The following example shows how to set an IP address of 10.1.1.100 and subnet mask of 255.255.255.0 for the management interface **Ethernet 1/0/0**:

```
<Huawei-AR-01> system-view
[Huawei-AR-01] interface ethernet 1/0/0          //Enter the interface view.
[Huawei-AR-01-Ethernet1/0/0] ip address 10.1.1.100 255.255.255.0
```

NOTE

The length of the subnet mask's binary notation is 24 (255.255.255.0 is equivalent to the binary value 11111111.11111111.11111111.00000000), so in this example you can replace 255.255.255.0 with 24.

2.4.4 User Interface Configurations

Basic concepts

If you log into a device through the console port, a console user interface is displayed. If you log in through Telnet, a virtual type terminal (VTY) user interface is displayed. To implement user control on the console port, for example, to set the user level to 2, you can run the following commands:

```
<Huawei> system-view
[Huawei] user-interface console 0          //Enter the console user interface.
[Huawei-ui-console0] user privilege level 2
```

Other users may also log into the device while you are logged into it. Each user has a separate user interface (the number of VTY interfaces supported varies depending on the device), so to differentiate multiple user interfaces, the device implements user interface numbering.

User interface numbering

When a user logs into a device, the device allocates to the user the lowest numbered idle user interface according to the login method used. User interfaces are numbered either relatively or absolutely.

- Relative numbering

The numbering format is user interface type + number. Generally, a device has one console port (some devices may have more) and 15 VTY user interfaces (5 VTY user interfaces enabled by default). When relative numbering is used, the ports are displayed as follows:

- Console user interface: CON 0
- VTY user interfaces: The first VTY user interface is VTY 0, the second VTY 1, and so on.

- **Absolute numbering**
An absolute number uniquely identifies a user interface. Absolute and relative numbers are in one-to-one mapping. The console user interface has a relative number of CON 0 and an absolute number of 0. A VTY user interface has a relative number ranging from VTY 0 to VTY 14 and an absolute number ranging from 129 to 143.

To check the user interfaces that a device supports, run the **display user-interface** command. For example:

```
<Huawei> display user-interface
  Idx   Type   Tx/Rx   Modem  Privi  ActualPrivi  Auth Int
+ 129   VTY 0   -       -      15    -            -   -
  130   VTY 1   -       -      15    -            A   -
  131   VTY 2   -       -      15    -            A   -
  132   VTY 3   -       -      15    -            A   -
  133   VTY 4   -       -      15    -            P   -
  134   VTY 5   -       -      15    -            P   -
  135   VTY 6   -       -      15    -            P   -
  136   VTY 7   -       -      15    -            P   -
  137   VTY 8   -       -      15    -            P   -
  138   VTY 9   -       -      15    -            P   -
  139   VTY 10  -       -      15    -            P   -
  140   VTY 11  -       -      15    -            P   -
  141   VTY 12  -       -      15    -            P   -
  142   VTY 13  -       -      15    -            P   -
  143   VTY 14  -       -      15    -            P   -
```

UI(s) not in async mode -or- with no hardware support:
1-128

- + : Current UI is active.
- F : Current UI is active and work in async mode.
- Idx : Absolute index of UIs.
- Type : Type and relative index of UIs.
- Privi: The privilege of UIs.
- ActualPrivi: The actual privilege of user-interface.
- Auth : The authentication mode of UIs.
 - A: Authenticate use AAA.
 - N: Current UI need not authentication.
 - P: Authenticate use current UI's password.
- Int : The physical location of UIs.

In the command output, the **Idx** column shows the absolute numbers, and the **Type** column shows the relative numbers.

User authentication

To ensure that only authorized users are allowed to access a device, the device supports password authentication and AAA authentication. None authentication is also supported.

- Password authentication
This mode is used by default and requires users to enter the correct login password. If no password is configured, login is denied.
- AAA authentication
This mode requires a correct user name and password combination. Using a user name and password combination improves security compared to password authentication. In addition, users are differentiated and do not affect each other during authentication. AAA authentication is generally used for Telnet logins because of its enhanced security.
- None authentication
This mode performs no authentication on users and is not recommended. None authentication allows users to log in directly without any login credentials.

The user authentication mechanism verifies user login. By default, after a user logs into a device using Telnet, the user is granted Level 0.

Example: configuring VTY user interfaces

During device commissioning, many users may log into the device to configure services. To limit the number of users who can log in through Telnet to 15, configure 15 VTY user interfaces. Then, to enable the users to configure services, set the user level to 2.

1. Set the maximum number of VTY user interfaces to 15.
Run the **user-interface maximum-vty** *number* command. Specify *number* as 15.

```
<Huawei> system-view  
[Huawei] user-interface maximum-vty 15
```
2. Enter the VTY user interface view.
Run the **user-interface vty** *first-ui-number* [*last-ui-number*] command. Specify *first-ui-number* as 0 and *last-ui-number* as 14 (relative numbers of VTY user interfaces). Note that [...] indicates that the enclosed parameter is optional; however, in this example, the parameter is required to limit the number of allowed users.

```
[Huawei] user-interface vty 0 14  
[Huawei-ui-vty0-14] //Enter the VTY user interface view.
```
3. Set the user level to 2 for the VTY user interface.
Run the **user privilege level** *level* command. Specify *level* as 2.

```
[Huawei-ui-vty0-14] user privilege level 2
```


4. Set the user authentication mode to AAA for the VTY user interface.
Run the **authentication-mode {aaa | none | password}** command.
[Huawei-ui-vty0-14] authentication-mode aaa
5. Configure a user name and password used in AAA authentication.
Exit from the VTY user interface view and run the **aaa** command to enter the AAA view. Run the **local-user user-name password cipher password** command to configure a user name and password (**cipher** indicates that the specified password is saved in ciphertext in the configuration file). Then, run the **local-user user-name service-type telnet** command to set the service type to Telnet.
[Huawei--ui-vty0-14] quit
[Huawei] aaa
[Huawei-aaa] local-user admin password cipher admin@123
[Huawei-aaa] local-user admin service-type telnet
[Huawei-aaa] quit
After the configuration is complete, the user name (admin) and password (admin@123) must be entered before the command interface is displayed.

Example: configuring the console user interface

Password authentication is used for console port logins. Generally, only administrators are allowed to log into a device through the console port, and therefore the highest user level is required.

1. Enter the console user interface.
Run the **user-interface console interface-number** command, where *interface-number* specifies the relative number of the console user interface. In this example, interface 0 is used.
[Huawei] user-interface console 0
2. Set the authentication mode and save the password in ciphertext.
Run the **authentication-mode {aaa | none | password}** command to configure an authentication mode, and run the **set authentication password cipher password** command to configure a ciphertext password.
[Huawei-ui-console0] authentication-mode password
[Huawei-ui-console0] set authentication password cipher admin@123

After the configuration is complete, save the configurations to the memory. To check the configurations, run the **display current-configuration** command. If the configurations are not saved, they will be lost after the device is powered off or restarted.

2.5 Configuration File Management

After completing this section, you should be able to:

- Understand the three basic concepts involved in file management.
- Save the current device configurations.
- Set the next startup configuration file.

2.5.1 Basic Concepts

To configure file management, you need to understand three concepts: current configurations, configuration file, and next startup configuration file.

1. Current configurations

The configurations in the device memory are the configurations that the device is currently running. When a device is powered off or restarted, the configurations in the memory are lost.

2. Configuration file

The configuration file contains the device configurations. Current configurations can be saved to this file, which is stored in an external storage device in either **.cfg** or **.zip** format. The configurations are loaded to device memory each time the device restarts. The configuration file can be queried, backed up, and even migrated to other devices. By default, the device saves the current configurations to **vrpcfg.zip**, which is stored in the root directory of the device's external storage device.

3. Next startup configuration file

The next startup configuration file is the file from which the device imports configurations upon restart. By default, the next startup configuration file is named **vrpcfg.zip**.

2.5.2 Saving the Current Configurations

The current configurations can be saved either manually or automatically.

1. Saving configurations manually

You can run the **save** [*configuration-file*] command at any time to save the current configurations to the configuration file specified by *configuration-file*. The specified configuration file must be in the **.cfg** or **.zip** format. If *configuration-file* is not specified, the configurations will be saved to the configuration file **vrpcfg.zip** by default.

To save the current configurations to the configuration file **vrpcfg.zip**, perform the following operations:

```
[Huawei] save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]:y           //Enter y to confirm the saving.
It will take several minutes to save configuration file, please wait...
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

To back up the configuration file **vrpcfg.zip** to **backup.zip**, perform the following operations:

```
[Huawei] save backup.zip
Are you sure to save the configuration to flash:/backup.zip?[Y/N]:y
Now saving the current configuration to the slot 17.
Save the configuration successfully
```

2. Saving configurations automatically

Autosaving configurations helps avoid configuration loss if they are forgotten to be manually saved. Autosaving can be performed either periodically or at a scheduled time.

Periodical autosaving enables the device to automatically save the configurations when a specified period elapses, regardless of whether the configurations have been changed. In contrast, scheduled autosaving enables the device to automatically save the configurations at a specified time every day. By default, autosaving is disabled.

To enable periodical autosaving, run the **autosave interval on** command, and then run the **autosave interval time** command to set an interval at which configurations are automatically saved. *time* specifies a time period, in minutes. The default value is 1440 min (24 h).

To enable scheduled autosaving, run the **autosave time on** command, and then run the **autosave time time-value** command to set a time at which configurations are automatically saved. *time-value* specifies a time, in the format of hh:mm:ss. The default value is 00:00:00.

The device saves the configurations to **vrpcfg.zip** or to the next startup configuration file if you have specified one for the next startup.

NOTE

The two autosaving modes, periodical and scheduled, cannot be used together. To use one autosaving mode, the other mode must be disabled. However, you can manually save the configurations at any time by running the **save** command, regardless of the autosaving mode in use.

2.5.3 Setting the Next Startup Configuration File

The **startup saved-configuration configuration-file** command allows you to specify the configuration file that a device uses upon restart. This next startup configuration file must be in either **.cfg** or **.zip** format and stored in the root directory (**flash:/**for example) of a device's external storage. *configuration-file* specifies a configuration file. If the specified configuration file does not exist in the root directory, an error will occur.

To specify the file **backup.zip** as the next startup configuration file, perform the following operations:

```
[Huawei] startup saved-configuration backup.zip
This operation will take several minutes, please wait...
Info: Succeeded in setting the file for booting system
```

The configurations in the specified file take effect only after the device restarts. By default, saving the current configurations will overwrite the configurations stored in the specified next startup configuration file.

Generally, devices are maintained by more than one engineer. As such, the current configurations may not be consistent with those in the specified next startup configuration file. To compare the current configurations against the next startup configuration file, you can run the **compare configuration** command. If the configuration commands differ, the device displays 120 characters (by default) starting from the line with differences.

For example, to compare the current configurations against the next startup configuration file **backup.zip**, perform the following operation:

```
[Huawei] compare configuration
The current configuration is not the same as the next startup configuration file.
===== Current configuration line 14 =====
undo http server enable
#
drop illegal-mac alarm
#
vlan batch 10 to 11
#
dot1x enable
mac-authen
#
set transceiver-monitoring disable
===== Configuration file line 14 =====
http server enable
#
drop illegal-mac alarm
#
vlan batch 10 to 11
#
dot1x enable
mac-authen
#
set transceiver-monitoring disable
```

The command output shows that line 14 differs between the current configurations and the next startup configuration file (the **undo http server enable** command is included in the current configurations, but is replaced with the **http server enable** command in the next startup configuration file). Then, you can determine whether to save the current configurations.

2.6 Remote Login Through Telnet

After completing this section, you should be able to:

- Understand the basic concepts of Telnet.
- Use Telnet to log into a device.

2.6.1 Introduction to Telnet

Telnet is an application-layer protocol in the TCP/IP model. This protocol enables a device (Telnet client) to log into a remote host (Telnet server) using TCP as the transport-layer protocol. Generally, the Telnet server listens for Telnet connections on TCP port 23.

A device that runs VRP can function as both a Telnet client and a Telnet server. For example, you can log into a device and use it as a Telnet client to telnet to another device. Figure 2.25 shows such a scenario, in which R1 functions as the Telnet server and the Telnet client for the PC and R2, respectively.

2.6.2 Logging into a Device Through Telnet

To log into a device from a PC running a Windows operating system, choose **Start > Run** and run the **telnet ip-address** command. For example, to log into a device whose IP address is 10.137.217.177, run the **telnet 10.137.217.177** command and click **OK** (Fig. 2.26).

In the displayed login dialog box, enter the user name and password. If the authentication is successful, the command line prompt <Huawei> will be displayed.

2.7 File Management

VRP uses a file system to manage all files and directories on a device. After completing this section, you should be able to:

- Understand the basic concepts of the file system.
- Back up a device's configuration file.
- Use TFTP and FTP to transfer files.

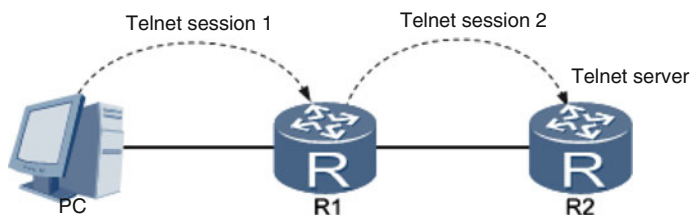


Fig. 2.25 Level-2 Telnet connection

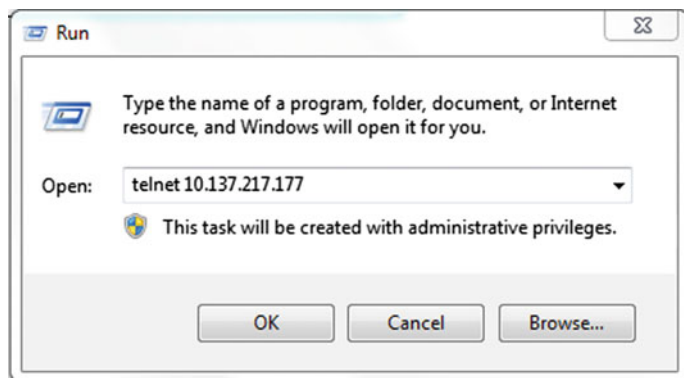


Fig. 2.26 CLI on the PC

- Delete files in a device.
- Configure the startup file of a device.

2.7.1 Basic Concepts

The VRP file system is used to create, delete, modify, copy, and display files and directories that are stored in a device's external storage, which for Huawei routers is flash memory and SD cards and for Huawei switches is flash memory and CF cards. Some devices also use external USB disks as supplementary storage devices.

An external storage device can store various types of files, including the configuration file, system software file, license file, and patch file. The system software file is the VRP operating system file and must be stored in **.cc** format in the root directory of the external storage device. The contents of this file are loaded to device memory and run when a device is powered on.

2.7.2 Backing up a Configuration File

In some scenarios such as a system upgrade, you may need to back up a device's configuration file to a specific folder in an external storage device. The following example describes the backup process, assuming that you have already logged into R1 through the PC (Fig. 2.27).

1. Locate the file to be backed up.

The **dir** [**/all**] [*filename* | *directory*] command displays files in a specified path. **all** indicates that all files and directories in the current path are displayed, including any files in the recycle bin. *filename* specifies a file. *directory* specifies a directory.

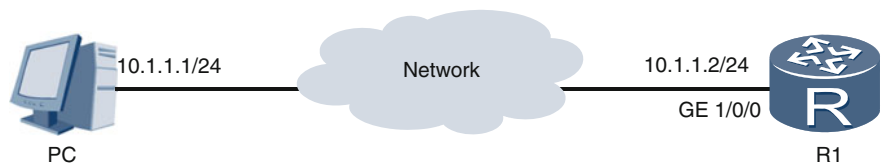


Fig. 2.27 Backing up a configuration file

To check files and directories in the root directory of R1’s flash memory, run the following command:

```
[Huawei] dir
Directory of flash:/

  Idx  Attr   Size(Byte)  Date           Time (LMT)      FileName
  ---  ---
0  -rw-   94,777,088  Jan 19 2013    16:20:29       software.cc
1  -rw-           0  Jan 28 2013    09:16:34       brdxpon_snmp_cfg.efs
2  -rw-       396  Jan 28 2013    09:18:27       rsa_host_key.efs
3  -rw-     1,317  Mar 20 2013    10:22:32       private-data.txt
4  -rw-    44,192  Mar 20 2013    10:26:25       mon_file.txt
5  -rw-       540  Jan 28 2013    09:18:26       rsa_server_key.efs
6  drw-      -    Jun 21 2012    10:25:25       cdr
7  -rw-     1,351  Mar 08 2013    13:55:28       vrpcfg.zip
8  -rw-   7,301,397  Jan 28 2013    09:18:26       abcd.zip
9  drw-      -    Aug 21 2012    11:21:58       dhcp

217,168 KB total (94,104 KB free)
<Huawei>
```

In this example, the configuration file **vrpcfg.zip** of 1351 bytes in size will be backed up.

2. Create a directory.

Run the **mkdir** *directory* command to create a directory. *directory* specifies the name of a directory (including its path) to be created. To create a directory **backup** in the root directory of a device’s flash memory, run the following command:

```
[Huawei] mkdir flash:/backup
Info: Create directory flash:/backup.....Done
```

3. Copy and rename the configuration file.

Run the **copy** *source-filename destination-filename* command to copy a file. *source-filename* specifies the path and name of a source file. *destination-filename* specifies the path and name of a destination file.

To copy the configuration file **vrpcfg.zip** to the directory **backup** and rename the file to **vrpcfgbak.zip**, run the following command:

```
[Huawei] copy vrpcfg.zip flash:/backup/vrpcfgbak.zip
Copy flash:/vrpcfg.zip to flash:/backup/vrpcfgbak.zip? (y/n) [n]: y
```

```
100% complete
```

```
Info: Copied file flash:/vrpcfg.zip to flash:/backup/vrpcfgbak.zip...Done
```

4. Check that the file has been backed up.

Run the **cd** *directory* command to change the current working directory. To check whether the configuration file has been successfully backed up, run the following commands:

```
[Huawei] cd flash:/backup
```

```
[Huawei] dir
```

```
Directory of flash:/backup/
```

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	1,351	Mar 20 2013	14:36:15	vrpcfgbak.zip

```
217,168 KB total (94,072 KB free)
```

```
<Huawei>
```

The command output shows that the directory **backup** contains the file **vrpcfgbak.zip**, meaning that the configuration file **vrpcfg.zip** has been backed up.

2.7.3 Transferring Files

1. TFTP

The Trivial File Transfer Protocol (TFTP) is a simple application-layer protocol in the TCP/IP model used to transfer files. It uses UDP as the transport-layer protocol with port 69.

TFTP works in the client/server model. Huawei routers and switches function only as TFTP clients. In Fig. 2.28, a PC functions as the TFTP server, and a router functions as the TFTP client. TFTP is used to transfer the VRP system software file on the PC to the router.

The **tftp** *tftp-server* {**get** | **put**} *source-filename* [*destination-filename*] command configures TFTP for file transfer. *tftp-server* specifies the IP address of a TFTP server. **get** indicates that a file is to be downloaded from a TFTP server to a TFTP client. **put** indicates that a file is to be uploaded from a TFTP client to a TFTP server. *source-filename* specifies a source file name. *destination-filename*

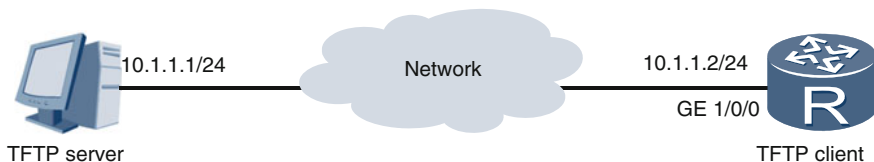


Fig. 2.28 Using TFTP to transfer a file

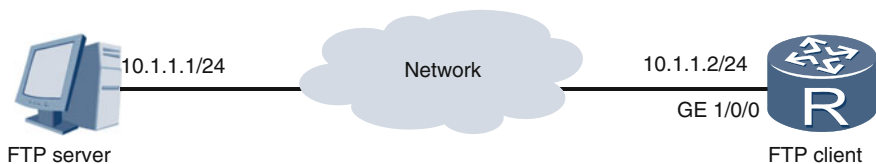


Fig. 2.29 Using FTP to transfer a file

specifies a destination file name. To download the VRP system software file **devicesoft.cc** from the PC to the router, run the following command:

```
[Huawei] tftp 10.1.1.1 get devicesoft.cc
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...\
TFTP: Downloading the file successfully.
93832832 bytes received in 722 seconds.
```

TFTP is easy to implement and use, but offers no security (for example, it does not verify user credentials or encrypt data). Anyone can upload or download files to or from TFTP servers, making TFTP suitable for file transfers only within secure network environments. For improved security, use FTP or SFTP.

2. FTP

Similar to TFTP, the File Transfer Protocol (FTP) is an application-layer protocol in the TCP/IP model. It uses TCP as the transport-layer protocol with port 21. Huawei routers and switches that run VRP can function as FTP servers as well as FTP clients. Compared to TFTP, FTP is more secure as it requires user credentials to establish an FTP connection. In addition, FTP allows you to delete files, and create and delete file directories on the FTP server.

In Fig. 2.29, a PC functions as the FTP server, and a router functions as the FTP client. FTP is used to transfer the VRP system software file on the PC to the router. Run the **ftp host-ip [port-number]** command to create an FTP connection. *host-ip* specifies the IP address of an FTP server. *port-number* specifies the port number of an FTP server. By default, TCP port 21 is used.

```
[Huawei] ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1: (none)):admin      //Specify the user name of the server.
331 Password required for admin.
Enter password:                  //Specify the password of the server.
230 User logged in.

[Huawei-ftp]
```

Run the **dir** command to check a list of files on the FTP server.

```
[Huawei-ftp] dir
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw-  1 ftp      ftp          0      Apr 17 10:53 back
drw-rw-rw-  1 ftp      ftp          0      Apr 17 10:53 backup
-rwxrwxrwx  1 noone    nogroup      0      Mar 23 15:49 aaa.cfg
-rwxrwxrwx  1 noone    nogroup    1351    Apr 02 20:37 vrpcfgbak.zip
-rwxrwxrwx  1 noone    nogroup   286620    Apr 07 08:56 sacrule.dat
-rw-rw-rw-  1 ftp      ftp      93832832    Mar 30 18:29 vrpsft.cc
8 File sent ok
FTP: 734 byte(s) received in 0.129 second(s) 5.68Kbyte(s)/sec.

[Huawei-ftp]
```

Similar to TFTP, FTP uses **get** and **put** keywords: **get** in the **get source-filename [destination-filename]** command indicates that a file is to be downloaded from an FTP server to an FTP client, and **put** in the **put source-filename [destination-filename]** command indicates that a file is to be uploaded from an FTP client to an FTP server.

In this example, the **get vrpsft.cc devicesoft.cc** command is run to download the VRP system software file **vrpsft.cc** from the FTP server (the PC) to the FTP client (the router) and rename the file **devicesoft.cc**.

```
[Huawei-ftp] get vrpsft.cc devicesoft.cc
200 Port command okay.
150 Opening ASCII mode data connection for vrpsft.cc.
226 Transfer complete.
FTP: 93832832 byte(s) received in 722 second(s) 560.70byte(s)/sec.
```

FTP transfers data in plaintext. For improved security, use the Secure File Transfer Protocol (SFTP) to transfer files. SFTP encrypts data and protects the integrity of the data being transferred.

2.7.4 Deleting a File

You may need to delete files occasionally to free up storage space. To do so, run the **delete [/unreserved] [/force] filename** command. **/unreserved** indicates that the file to be deleted cannot be restored. **/force** indicates that no confirmation is required to delete the specified file. *filename* specifies the name of a file to be deleted.

If **/unreserved** is not configured, the file to be deleted is moved to the recycle bin and can be restored using the **undelete** command. The file will still occupy

storage space inside the recycle bin. The **reset recycle-bin** command deletes all files in the recycle bin. Once files are deleted from the recycle bin, they cannot be restored.

To permanently delete a file, for example, **abcd.zip**, perform the following operations:

```
[Huawei] delete /unreserved abcd.zip
Warning: The contents of file flash:/backup/abcd.zip cannot be recycled.
Continue? (y/n) [n]:y
Info: Deleting file flash:/backup/abcd.zip...
Deleting file permanently from flash will take a long time if
needed.....succeed.
```

2.7.5 Setting a System Startup File

Startup files include the system software file and other files loaded from an external storage device to the memory for the device startup. Before setting the next startup file, run the **display startup** command to check the startup files used for the next startup.

```
[Huawei] display startup
MainBoard:
  Startup system software:          flash:/software.cc
  Next startup system software:     flash:/software.cc
  Backup system software for next startup:  null
  Startup saved-configuration file:   flash:/vrpcfg.zip
  Next startup saved-configuration file:  flash:/vrpcfg.zip
  Startup license file:             null
  Next startup license file:        null
  Startup patch package:           null
  Next startup patch package:       null
  Startup voice-files:              null
  Next startup voice-files:         null
```

The command output shows that the system software file **software.cc** will be used for the next startup of the device. The **startup system-software system-file** command sets the system software file for the next startup. *system-file* specifies the file. To use the file **devicesoft.cc** for the next startup, run the following command:

```
[Huawei] startup system-software devicesoft.cc
This operation will take several minutes, please wait...
Info: Succeeded in setting the file for booting system
```

To verify whether the setting has taken effect, run the **display startup** command.

```
[Huawei] display startup
MainBoard:
  Startup system software:          flash:/software.cc
  Next startup system software:     flash:/devicesoft.cc
  Backup system software for next startup: null
  Startup saved-configuration file:  flash:/vrpcfg.zip
  Next startup saved-configuration file: flash:/vrpcfg.zip
  Startup license file:             null
  Next startup license file:        null
  Startup patch package:            null
  Next startup patch package:       null
  Startup voice-files:              null
  Next startup voice-files:         null
```

The command output shows that the system software file for the next startup has been set to **devicesoft.cc**.

2.8 Basic Configuration Commands

Some commands are used more frequently than others and so are worth remembering. Table 2.4 lists some of the basic configuration commands that are most frequently used.

Table 2.4 VRP basic configuration commands

Command	Description
authentication-mode {aaa password none}	Sets an authentication mode for login to a user interface
autosave interval {value time configuration time}	Sets periodical autosaving
autosave time {value time-value}	Sets scheduled autosaving
cd directory	Changes the working directory
clock datetime HH:MM:SS YYYY-MM-DD	Sets the current date and time
clock timezone time-zone-name {add minus} offset	Sets a local time zone
compare configuration [configuration-file] [current-line-number save-line-number]	Compares the current configurations against the next startup configuration file
copy source-filename destination-filename	Copies a file
delete [/unreserved] [/force] {filename devicename}	Deletes a file
dir [/all] [filename directory]	Displays all files and directories or a specified file or directory

(continued)

Table 2.4 (continued)

Command	Description
display current-configuration	Displays the current configurations
display startup	Displays the system startup file
display this	Displays the running configurations in the current view
display user-interface <i>[ui-type ui-number1 ui-number]</i> [summary]	Displays the user interface
ftp <i>host-ip [port-number]</i>	Configures a device to establish a connection with an FTP server
get <i>source-filename [destination-filename]</i>	Downloads a file from a server to a client
local-user <i>user-name</i> password cipher <i>password</i>	Creates a local user and sets a password
local-user <i>user-name</i> service-type telnet	Configures the access type for a local user
mkdir <i>directory</i>	Creates a directory
move <i>source-filename destination-filename</i>	Moves a source file to a destination directory
put <i>source-filename [destination-filename]</i>	Uploads a file from a client to a server
quit	Returns to the upper-level view, or quits the system if the current view is the user view
reboot	Reboots a device
reset recycle-bin	Deletes files in the recycle bin permanently
save	Saves the current configurations
schedule reboot {at time delay interval}	Configures scheduled restart of a device
startup saved-configuration <i>configuration-file</i>	Sets a next startup configuration file
sysname <i>host-name</i>	Sets a host name for a device
system-view	Displays the system view from the user view
telnet <i>host-name [port-number]</i>	Enables a device to use Telnet to log into another device
tftp <i>tftp-server {get put} source-filename [destination-filename]</i>	Uploads a file to or downloads a file from a TFTP server
user-interface <i>[ui-type] first-ui-number [last-ui-number]</i>	Displays one or more user interfaces
user-interface maximum-vty <i>number</i>	Sets the maximum number of login users
user privilege level <i>level</i>	Sets a user level

2.9 Review Questions

1. What is VRP? (Choose all that apply)
 - A. A network operating system
 - B. System software
 - C. A network device
 - D. A software platform applicable to multiple network devices
2. Which prompt indicates the interface view? (Choose one)
 - A. <Huawei>
 - B. [Huawei]
 - C. [Huawei-GigabitEthernet0/0/1]
 - D. [Huawei-Vlan1]
3. Which of the following VRP command levels can Level-2 users run? (Choose one)
 - A. Levels 0 and 1
 - B. Levels 0, 1, and 2
 - C. Level 2
 - D. Levels 0, 1, 2, and 3
4. What is the default FTP port number? (Choose one)
 - A. 23
 - B. 69
 - C. 21
 - D. 24
5. What configurations must be performed after you log into a device for the first time? (Choose all that apply)
 - A. Set a host name.
 - B. Set the system time.
 - C. Set a device IP address.
 - D. Set a user interface.



<http://www.springer.com/978-981-10-1553-3>

HCNA Networking Study Guide

Huawei Technologies Co., Ltd. (Ed.)

2016, XXVI, 342 p. 242 illus., 168 illus. in color.,

Hardcover

ISBN: 978-981-10-1553-3